UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/691,428	10/21/2003	Gerard Anthony Brady	12832/100188	9179

21323 7590 07/24/2007

TESTA, HURWITZ & THIBEAULT, LLP
HIGH STREET TOWER
125 HIGH STREET
BOSTON, MA 02110

EXAMINER	
ABEDIN, SHANTO	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
07/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/691,428	BRADY ET AL.	
	Examiner	Art Unit	
	Shanto M Z Abedin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 May 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) *16-33* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/21/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to communications filed on 05/01/2007.

2. The applicant's election of claims 1-15 without traverse in response to the previous restriction/ election requirement is acknowledged.

3. Claims 1- 33 are now pending in the application.

4. Claims 1-15 have been presented for the examination.

5. Claims 1-15 have been rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-15 are rejected under 35 USC 102 (e) as being anticipated by Graham et al (US 7237264 B1).

Regarding claims 1 and 15, Graham et al discloses a method for analyzing a security event in a distributed fashion, comprising:

(a) detecting an occurrence of a security event within a customer network (Col 5, starts at line 55; Claim 1; detecting alert/ suspicious condition/ signatures etc);

(b) querying a first component of the customer network for data in response to the detected occurrence of the security event (Col 8, starts at line 5; Col 13, starts at line 6; Claim 1; request/ response from target, or acquiring aggregation level or ranked value);

(c) receiving, by a data monitor located within the customer network, first data from the component in response to the query (Col 4, starts at line 50; Col 13, starts at line 6);

(d) determining, based on the received first data, whether to query for additional data (Col 4, starts at line 50; each of these variables alone or in combination, may dictate the type and extent of a response; Col 13, starts at line 6; analysis);

(e) querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step (Col 4, starts at line 50; Col 12, starts at line 50; Claim 1; query/ acquiring additional/ new/ contextual information from suspect, or suspect's gateway; acquiring combination of alert signature and contextual information; one or more variables related to the alert type and condition)

(f) analyzing the security event using at least one of the first data and the additional data (Col 4, starts at line 50; Col 12, starts at line 50; Claim 1-12; analyzing and assigning alerts/ condition).

Regarding claim 2, Graham et al discloses the method of claim 1 wherein step (a) further comprises determining at least one of intrusion of the customer network, a port scan, service probes, a signature from an attack, a buffer overflow attempt, a format string attack, a

denial of service attempt, a web-based attack, and an attempted rights escalation (Col 6, starts at line 55; Col 9, starts at line 50; port scan; buffer overflow; signature attack etc).

Regarding claim 3, Graham et al discloses the method of claim 1 wherein step (a) further comprises monitoring the customer network for the security event (Col 4, starts at line 40; Col 13, starts at line 6; claims 19,28,31; monitoring).

Regarding claim 4, Graham et al discloses the method of claim 1 wherein step (a) further comprises determining at least one of nature of the security event, likelihood that the security event is harmful, and impact of the security event (Col 6, starts at line 55; Col 9, starts at line 50; claims 19, 28, 31; monitoring/ determining attacks/ alerts).

Regarding claim 5, Graham et al discloses the method of claim 1 wherein step (a) further comprises detecting, by the data monitor, the occurrence of the security event. (Col 9, starts at line 50; claims 19, 28; monitoring/ determining attacks/ alerts).

Regarding claim 6, Graham et al discloses the method of claim 1 wherein the security event further comprises a potential security event (Col 6, starts at line 55; Col 9, starts at line 50; claims 19, 28, 31).

Regarding claim 7, Graham et al discloses the method of claim 1 wherein at least one of the first component and the another component of the customer network further

comprises at least one of the data monitor and a client computer (Col 4, starts at line 30; Col 12, starts at line 50).

Regarding claim 11, Graham et al discloses the method of claim 1 wherein step (d) further comprises determining, by the data monitor, whether to query for additional data (Col 4, starts at line 50; Col 12, starts at line 50; Claim 1; query/ acquiring additional/ new/ contextual information from suspect, or suspect's gateway; acquiring combination of alert signature and contextual information).

Regarding claim 12, Graham et al discloses the method of claim 1 wherein step (f) further comprises populating a trouble ticket during the analysis (Col 12, starts at line 50; Claim 1; assigning alert conditions and rank value; the examiner interprets Graham et al 's teachings of assigning alert conditions and rank value as assigning trouble ticket based on the analysis).

Regarding claims 8-10 and 13-14, they recite the limitations of claims 1-7, therefore, they are rejected applying as same as applied rejecting claims 1-7.

Conclusion

7. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

AU 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

7, 20, 07